加餐5 | 安全新技术：IoT、IPv6、区块链中的安全新问题

2020-02-28 何为舟

安全攻防技能30讲 进入课程 >

讲述：何为舟
时长 09:45 大小 7.83M

你好，我是何为舟。欢迎来到安全专栏的第 5 次加餐时间。

随着科技的快速发展，各种新的技术和概念不断出现，持续出现的新技术会不断推动安全的发展。虽然，每一个新技术都会衍生出新的安全威胁和隐患，但是，这些新的安全问题也正是安全行业保持活力的源泉。所以，对于安全人员来说，这些新技术的出现既是一种挑战，也是一种机遇。

近几年，IoT、IPv6 和区块链是三个热度很高的新技术，我也最常听到三个热词。今天我们就一起来探讨一下，这几个新技术都面临哪些独特的安全问题。

独特的 IoT 安全

毫无疑问，IoT（Internet of Things，物联网）是最近十年来比较火热的一个技术。对比于当前的网络环境，IoT 的网络主要有以下几个特点：

设备更多：每一件小的物品都有可能成为联入互联网的设备

设备性能更低：受限于体积和供电量，单台设备能够搭载的硬件配置都不高

更加开放：由于设备的数量和类型众多，无法统一标准，因此 IoT 的 网络环境也更加开放

那么，这些特点会给安全性带来哪些新的挑战呢？关于这个问题，我推荐你玩一玩《看门狗》这款游戏，它很好地描绘了一个未来 IoT 城市中会面临的各类安全问题。那在此之前，我先和你分享一下我对这些新挑战的思考。

我认为最明显的问题就是认证更加复杂了。

在使用电脑或者手机连入网络的时候，我们可以手动输入密码来完成认证。但是，当我们想要将各类小硬件连入网络的时候，没有键盘和屏幕可以供我们输入密码。为了解决这个认证问题，目前小米等 IoT 厂商的解决方案是，先让手机直接控制设备，配置好 WiFI 密码后，再让设备连入网络。

但是，这其实又引发了一个新的问题，如何确认是你本人在控制设备，而不是黑客呢？针对这个问题，现在也有对应的解决方案，那就是在短时间内开放设备的控制权限，限制手机在这个时间内完成对设备的控制。

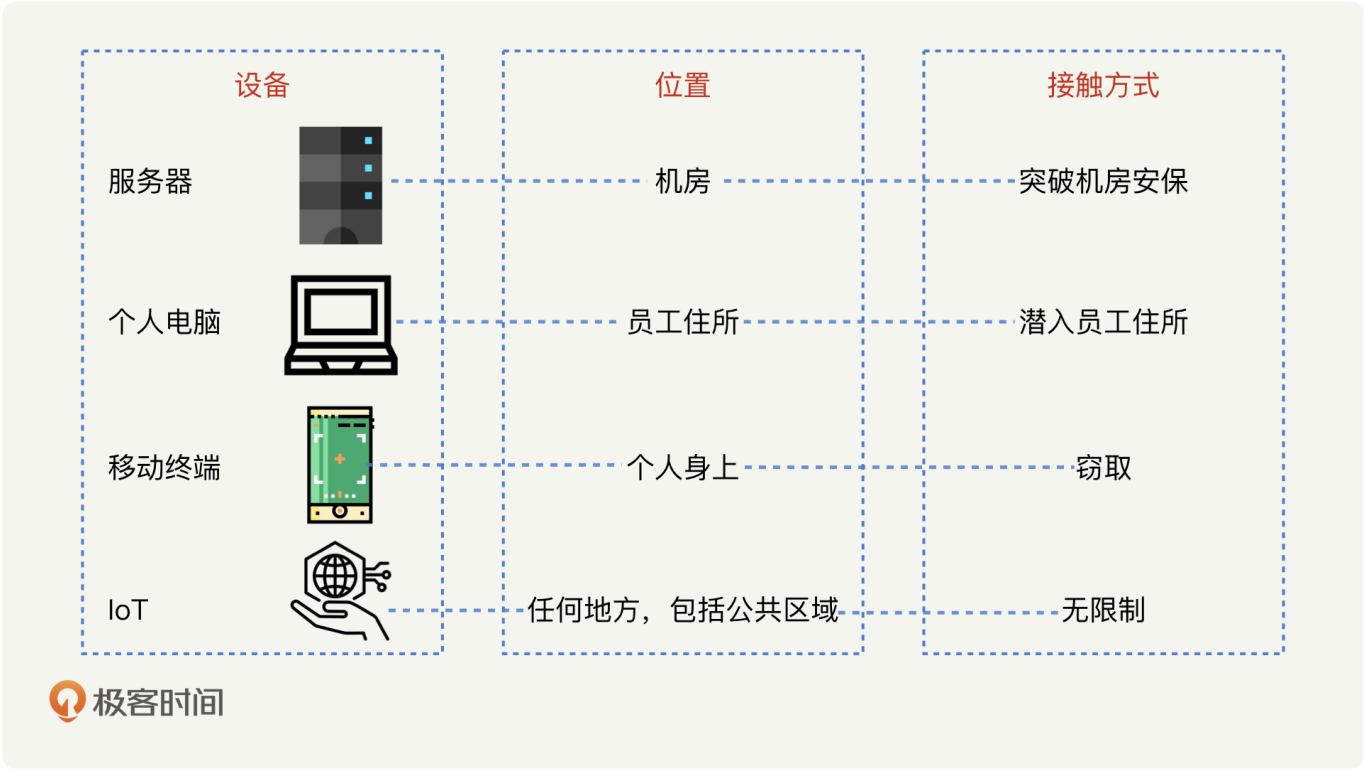
仔细观察的话，你会发现这个解决方案有一个假设前提：黑客没办法在短时间内发现并控制设备。在当前的环境下，这个前提是成立的。但是随着技术的发展，IoT 设备可能充斥在我们身边的每一个角落里，当有一个设备被黑客控制了之后，它很可能会时刻监控这周围的环境，一旦发现其他的设备开放控制权限，就会立即黑入。可以说，通过这样的攻击方式，任何一个设备都有可能被黑客所控制。

因此，**如何确保 IoT 中设备与网络、设备与设备之间的通信是可信的**，是未来认证技术需要面临的主要挑战之一。

其次，我认为物理攻击会越来越流行。

物理攻击实际上是安全领域内的**降维打击。** 换句话说，当底层的硬件被黑客控制之后，我们就无法保障运行在硬件之上的系统和软件的安全性了。

IoT 的发展，事实上正让物理攻击变得越来越容易。我总结了一张物理攻击的发展过程图，你可以看到，随着 IoT 越来越小、越来越智能，和我们的联系越来越紧密，物理攻击的难度也变得越来越低。在未来，公共区域内的所有设备甚至都有可以成为黑客的囊中之物。



因此，**如何对物理攻击进行有效的防控**，也是未来安全中需要解决的主要挑战之一。

除了带来新的安全挑战，IoT 能够造成的安全威胁也变得更加复杂了。

目前来说，黑客利用 IoT 设备发起的最主要的攻击还是 DDoS 攻击，即黑客利用海量的 IoT 设备向目标服务器发送巨大的网络流量，导致服务器无法响应正常请求。

随着 IoT 的发展，黑客能够控制的设备越来越多，能够导致的影响也会越来越大。你一定在很多电影中看到过类似的情景，比如，黑客通过操纵汽车控制医疗设备等方式，导致人员伤亡。

因此，**如何保护 IoT 设备免受黑客的攻击**，同样会成为未来安全的主要挑战之一。

IPv6 对安全的影响

因为 IPv4 的地址空间短缺问题，IPv6 是国家重点推进的一个技术方向。目前三大运营商已经完成了改造，各大互联网公司也已经接到了兼容 IPv6 的强制要求，我相信国内应该会很快推广和普及 IPv6。

IPv6 和 IPv4 相比最大区别就是 IP 地址变得非常庞大了。那么，庞大的 IP 地址对于安全来说，又意味着什么呢？

我认为对于黑客来说，最大的影响就是**网络扫描不再可能**。

我们知道，找到攻击目标是黑客发起攻击的第一步。因此，很多黑客会通过扫描网络来发现目标。目前，性能最优的扫描工具是 Masscan，它能够在 5 分钟内扫遍全部 IPv4 的地址空间。

而 IPv6 的地址空间是 IPv4 的 2^96 倍，黑客想要利用现有的扫描工具快速遍历 IPv6 的地址空间，显然是不可能的。因此，黑客就只能通过其他方式去精准定位目标了。

除了对黑客有影响以外，**庞大的 IP 地址对公司安全来说，也同样是一种负担**。

IP 地址变多就意味着黑客手中的 IP 资源变多了，同时，IPv6 的高变化频率还会让同一个设备的 IP 经常性的发生变化。因此，使用了 IPv6 之后，我们就很难利用黑名单对 IP 进行标记和处罚了。

另外，仍然有待观察的一点是，**IPv6 的复用性是否会比 IPv4 更低**。

IPv4 由于地址匮乏，有很高的复用性（一个学校可能都在共用一个 IP 地址），这让我们很难根据 IP 去定位到一个具体的位置或者人。

而 IPv6 的地址空间是足够的（每一粒沙子都能分配到一个 IP 地址），因此，IP 复用就不再是一个刚需了。所以，如果 IPv6 的复用性远低于 IPv4 的话，就能让 IP 的定位变得更准确。那么对于安全工作来说，想要找到黑客也会更加容易。

区块链中的安全问题

最后，我们再来聊一聊近两年兴起的区块链。目前，区块链最成功的应用形式，就是以比特币为代表的各类虚拟货币。那么，比特币和区块链的安全性如何呢？它们又面临什么样的安

全威胁呢？下面，我们一起来看。

我们都知道，区块链的思想是去中心化，即将数据和算力分散到每一个小的计算节点中，最终，以少数服从多数的形式来完成数据的计算和存储。这实际上是一种对完整性的保障。这么说你可能还不理解，我举个例子。

以货币为例，我们现在通过支付宝、微信等电子货币来完成日常交易，事实上是将钱交由支付宝和微信这样的中心机构进行集中保管。而对于支付宝、微信来说，理论上是可以对用户的余额进行篡改的，不过，因为受到了多方面限制，这一操作是无法实现的。

但是在比特币中，因为不存在中心机构，每个用户的余额由所有人共同保管，因此没有任何一个节点可以实现篡改。

但如果你仔细想想的话，就会发现这种近乎完美的完整性保障，是通过牺牲机密性来完成的。也就是说，在支付宝中，你无法知道其他用户的余额，但是在比特币中，每一笔交易和每一个用户的余额都是公开的信息，因此比特币不提供任何针对机密性的保护措施（比如，你可以在blockchain看到所有的比特币信息）。

尽管比特币本身的完整性无可挑剔，但仍然无法阻止由于用户个人密钥丢失而导致的资产损失。这就好比你安装了一个特别结实的门，但只要钥匙丢了，门的存在就毫无意义了。事实上，目前大部分的比特币安全事件，都是黑客成功盗取了用户或者公司系统的比特币密钥之后，再去盗取对应账号的余额。

另外，比特币是目前黑客们主要使用的货币之一。其原因在于，它是匿名的（注意：匿名不是机密性，匿名是指你无法通过比特币的账号，关联到某个具体的人）。这也就保证了，即使警方知道了黑客的账户，也没办法抓到黑客。而且，由于比特币的去中心化，警方也没办法封停黑客的账户，追回被盗的比特币。

所以，比特币这样一种去中心化且匿名的货币体系，既不保险，也不利于政府的管控，因此国内对于以区块链为基础的电子货币落地，始终不认可。

总结

今天，我们主要对 IoT、IPv6 和区块链这三个热门技术及其安全性进行了盘点。这些新的技术都具备其独特的应用场景，也都带有独特的安全问题。这些问题既可能是这些技术本身

所存在的一些缺陷，也可能是对已有的安全防御工作产生的威胁。

我们不仅要对这些新技术进行持续的关注，还要思考它们会产生的新安全需求，然后去学习对应的新知识。这也是安全人员提升自我价值，保持思维活力的有效手段。

思考题

最后，咱们来看一道思考题。

除了我们今天讲的这三种技术，你还接触过哪些新的技术呢？不妨和我的一样，把你对这些新技术的安全思考都写下来。

欢迎留言和我分享你的思考和疑惑，也欢迎你把文章分享给你的朋友。我们下一讲再见！

课程学习计划

关注极客时间服务号
每日学习签到

月领 25+ 极客币

【点击】保存图片，打开【微信】扫码>>>

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇　加餐4 | 个人成长：学习安全，哪些资源我必须要知道？

精选留言 (3)

写留言

许童童

2020-02-29

通过这篇文章开阔了我的视野。

展开

carrycoder

2020-02-28

连续用一周的时间刷完了这个专栏，收获很大，作为开发人员之前对安全的知识都是零零散散，看完这个专栏对安全有了一个初步体系化的认识和了解，在日常开发中也培养了思考应用程序安全问题的意识，收获很大，谢谢老师精彩的分享

展开

leslie

2020-02-28

物联网宣传的很广泛：可是安全性是一个极大的问题，只要联网的设备都可能存在安全隐患：尤其是现在几乎所有的APP都要求取得用户的摄像头和存储权限，你永远不知道你的摄像头是否被人使用，尤其是当你的手机没在使用存储或摄像头时。
IPV6：好的一面是定位准确了，不好的一面是管理起来更麻烦了。
区块链：个人觉得最大的特色是非重复性，比特币最大的特点是创造困难而非查询困难...

展开